ON THE CYCLOTOMIC FUNCTION.*

By DR. L. E. DICKSON, The University of Chicago.

1. If $p^n=1$ and $p^m\neq 1$ $(m<n)$, p is called a primitive nth root of unity. Let $Q_n(x)$ be the equation whose roots are the various nth primitive roots of unity without repetition. Let $n=\nu p^r$, ν not being divisible by the prime p. We first prove that

$$(1)\qquad Q_n(x)=Q_\nu(x^{p^r})\div Q_\nu(x^{p^{r-1}}).$$

To show that the division is exact, let $\xi_1, \ldots, \xi_e$ be the distinct νth roots of unity. Then $\xi_1{}^p, \ldots, \xi_e{}^p$ differ only as to order from $\xi_1, \ldots, \xi_e$. Hence

$$Q_\nu(x^{p^r})=\prod_{i=1}^{e}(x^{p^r}-\xi_i{}^p),\quad Q_\nu(x^{p^{r-1}})=\prod_{i=1}^{e}(x^{p^{r-1}}-\xi_i).$$

Since $y-\xi$ divides $y^p-\xi^p$, the division (1) is exact. If the value x makes the quotient vanish, then $(x^{p^r})^m=\xi_i{}^m=1$ if and only if m is a multiple of ν, while $x^{\nu p^{r-1}}\neq 1$; hence x is a primitive nth root of unity.

We employ (1) as a recursion formula to determine $Q_n(x)$. As a permanent notation, set $n=p_1{}^{r_1}\,p_2{}^{r_2}\ldots p_s{}^{r_s}$, where $p_1, \ldots, p_s$ are distinct primes. Then

$$(2)\quad Q_n(x)=Q_\mu(x^{p_1^{r_1}p_2^{r_2}})\,Q_\mu(x^{p_1^{r_1-1}p_2^{r_2-1}})\div Q_\mu(x^{p_1^{r_1}p_2^{r_2-1}})\,Q_\mu(x^{p_1^{r_1-1}p_2^{r_2}}),$$

where $\mu=n\div p_1{}^{r_1}p_2{}^{r_2}$. In general, for $N=p_1{}^{r_1}p_2{}^{r_2}\ldots p_\sigma{}^{r_\sigma}$, we get

$$(3)\qquad Q_n(x)=\frac{Q_{n/N}(x^N)\ \Pi Q_{n/N}(x^{N/p_ip_j})\ldots}{\Pi Q_{n/N}(x^{N/p_i})\ \Pi Q_{n/N}(x^{N/p_ip_jp_k})\ldots},$$

in which $i, j, \ldots$ range from $1, \ldots, \sigma$. Now $Q_1(x)=x-1$. For $\sigma=s$, $N=n$, and (3) becomes

$$(4)\qquad Q_n(x)=\frac{(x^n-1)\ \Pi(x^{n/p_ip_j}-1)\ldots}{\Pi(x^{n/p_i}-1)\ \Pi(x^{n/p_ip_jp_k}-1)\ldots},$$

where in the denominator the products extend over the combinations 1, 3, 5, ... at a time of $p_1, \ldots, p_s$; in the numerator, 2, 4, ... at a time.

Conversely, (1) follows from (4). The terms of (4) in which p_1 does not enter explicitly combine into $Q_\nu(x^{p_1^{r_1}})$; those in which p_1 enters explicitly combine into $1\div Q_\nu(x^{p_1^{r_1-1}})$.

*Read before the American Mathematical Society, Chicago, April 22, 1905.

2. The usual proof* of (4) is essentially only a verification. Since $Q_d(x) = 0$ gives all the primitive dth roots of unity withour repetition, we have

$$(5) \qquad x^n - 1 = \Pi Q_d(x), \quad x^{n/p_1} - 1 = \Pi Q_\delta(x), \ldots\ldots$$

where d ranges over all the divisors of n; δ over those of n/p_1. When the products (5) are substituted in the second member of (4), every Q cancels except Q_n. In fact, if $d = p_1^{a_1} \ldots\ldots p_t^{a_t} p_{t+1}^{r_{t+1}} \ldots\ldots p_s^{r_s}$, where $t > 0$ and each $a_i < r_i$, Q_d divides exactly $A = 1 + {}_tC_2 + {}_tC_4 + \ldots\ldots$ terms of the numerator of (4) and exactly $B = {}_tC_1 + {}_tC_3 + \ldots\ldots$ terms of the denominator, ${}_tC_k$ being the number of combinations of t things k at a time. But $A - B = (1-1)^t = 0$.

3. From equation (4) follows as a corollary the important formula

$$(6) \qquad \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots\ldots (1 - \frac{1}{p_s}),$$

where $\phi(n)$ denotes the number of positive integers not greater than n and relatively prime to n. Indeed, if ρ is a primitive nth root of unity, ρ^m is likewise if and only if m is relatively prime to n. But the degree of (4) evidently equals the right member of (6).

It follows from (4) that the polynomial $Q_n(x)$ has integral coefficients.

There are various proofs of the theorem that $Q_n(x)$ is algebraically irreducible, *i. e.*, can not be expressed as a product of polynomials in x with rational coefficients.†

4. Theorem. *For an integer x, the greatest common divisor g of $Q_n(x)$ and $x^{n/p_1} - 1$ is* 1 *or p_1. If $g = p_1$, Q_n is not divisible by p_1^2 unless $n = p_1 = 2$, $x \equiv 3$ (mod4), whence $Q_n = x + 1$.*

Dividing the first equation (5) by the second, we get

$$(7) \qquad (x^{n/p_1})^{p_1 - 1} + (x^{n/p_1})^{p_1 - 2} + \ldots\ldots + x^{n/p_1} + 1 = Q_n(x).P(x),$$

$P(x)$ being a polynomial in x with integral coefficients. When the left member of (7) is divided by $x^{n/p_1} - 1$, the remainder is 1 or p_1. Hence $g = 1$ or p_1.

Let $g = p_1$, so that $x^{n/p_1} - 1 = kp_1$, k an integer. Substituting $kp_1 + 1$ for x^{n/p_1} in (7), we obtain $p_1 + \frac{1}{2}p_1(p_1 - 1)kp_1 +$terms in p_1^2. This is not divisible by p_1^2 if $p_1 > 2$, nor if $p_1 = 2$ and k is even. If $p_1 = 2$ and $k = 2l + 1$, then $x^{n/2} = 4l + 3$, whence $n/2$ must be odd and $x \equiv 3$ (mod4). Suppose that $n > 2$ and $n/2 = p^r p_3^{r_3} \ldots\ldots p_s^{r_s} = m =$odd. Performing in (4) the divisions of the type $(x^{2a} - 1) \div (x^a - 1)$, we get

$$(8) \qquad \frac{x^m + 1}{x^{m/p} + 1} \cdot \prod_{i=3}^{s} \frac{x^{m/p\,p_i} + 1}{x^{m/p_i} + 1} \cdot \prod_{i,j=3}^{s} \frac{x^{m/p_i p_j} + 1}{x^{m/p\,p_i p_j} + 1} \cdot \prod_{i,j,k} \frac{x^{m/p\,p_i p_j p_k} + 1}{x^{m/p_i p_j p_k} + 1} \ldots\ldots$$

*On the general principle of the inversion involved, see Dedekind, *Crelle*, Vol. 54 (1857), pp. 1-26; Dirichlet-Dedekind, *Zahlentheorie*, p. 362; Bachmann, *Kreistheilung*, 1872, pp. 8-11, 16, and *Zahlentheorie*, I, pp. 40-42.

†See Bachmann, *Kreistheilung* (Leipzig. Teubner, 1872), pp. 31-43.

Since the exponents are all odd, each fraction or its inverse equals $1+f$, f containing an even number of powers of x. Hence Q is odd (cf. §5).

5. Theorem. *For $n=p_1^{r_1}.....p_s^{r_s}$ and x an integer, $Q_n(x)$ is divisible by p_1 if and only if x belongs to the exponent $\nu=n/p_1^{r_1}$ modulo p_1; in the contrary case,* $Q_n(x)\equiv 1$ *(mod p_1).*

By Fermat's theorem, $x^{p_1}\equiv x$ (mod p_1). Hence by (1), $Q_n(x)\equiv 1$ (mod p_1) unless $Q_v(x)\equiv 0$. Now $Q_v(x)$ divides algebraically the function

$$(x^v-1)\div(x^{v/p_i}-1)=(x^{v/p_i})^{p_i-1}+.....+x^{v/p_i}+1 \qquad (1<i\leqq s).$$

Hence if $x^{v/p_i}\equiv 1$ (mod p_1), there is an integer k such that $kQ_v(x)\equiv p_i$ (mod p_1); whence Q_v is not congruent to 0 (mod p_1). There remains the case in which x^{v/p_i} is not congruent to 1 (mod p_1) for $i=2$, ..., s. If $x^v\equiv 1$ (mod p_1), x belongs to the exponent ν modulo p_1 and $Q_v\equiv 0$; if $x^\nu-1$ is not congruent to 0, its divisor Q_ν is not congruent to 0 (mod p_1).

Example. For $n=2.3.7$, formula (8) gives

$$Q_{42}(x)=\frac{(x^{21}+1)\,(x+1)}{(x^7+1)\,(x^3+1)}=x^{12}+x^{11}-x^9-x^8+x^6-r^4-x^3+x+1.$$

Thus $Q_{42}\equiv 1$ (mod 2 or 3); $Q_{42}(x)\equiv 1$ (mod 7) if $x\equiv 0$, -1 or $x^3\equiv +1$; but $Q_{42}(x)\equiv 0$ (mod 7) if $x^2-x+1\equiv 0$ (mod 7), *i. e.*, if x belongs to the exponent $\nu=6$.

Corollary. No one of the prime factors of n except the greatest can divide $Q_n(x)$.

6. Theorem. *If x is a positive integer >1, $Q_n(x)$ has a prime factor not dividing x^m-1 $(m<n)$, except in the cases $n=2$, $x=2^k-1$ $(k\geqq 2)$; and $n=6$, $x=2$.*

If $n=p^r$, $Q=y^{p-1}+.....+y+1>p$, where $y=x^{p^{r-1}}$, so that the theorem follows from §4. We suppose henceforth that $n=p_1^{r_1}.....p_s^{r_s}$, $s\geqq 2$.

In view of §1, $Q_n=A/B$, where

$$A=\frac{x^n-1}{x^{n/p_1}-1}\,.\,\Pi\frac{x^{n/p_ip_j}-1}{x^{n/p_1p_ip_j}-1}.....,\ B=\Pi\frac{x^{n/p_i}-1}{x^{n/p_1p_i}-1}\,.\,\Pi\frac{x^{n/p_ip_jp_k}-1}{x^{n/p_1p_ip_jp_k}-1}.....,$$

in which i, j, k, ... run from 2 to s. Now $x^{a(k-1)}<(x^{ka}-1)\div(x^a-1)<2x^{a(k-1)}$. Hence $Q_n>\alpha/\beta$, where α is the result of retaining only the first term of each division in A, β the result of taking twice the first term of each division in B. The number of factors 2 introduced in B is ${}_{s-1}C_1+{}_{s-1}C_3+.....=2^{s-2}$. The exponent of x in α/β is evidently the degree $\phi(n)$ of Q_n. Let $x^{n/p_1p_2\cdots p_s}=y$. Hence

$$Q_n(x)>y^{(p_1-1)\ldots(p_s-1)}\div 2^{2^{s-2}},$$

y an integer>1. In view of § §4-5, it suffices to prove that $Q_n>p_1$, the greatest of the primes p_i, the case $n=6$, $x=2$ being an exception. For $s>2$, we have $p_1\geqq 5$, $y^{p_1-1}>2p_1$, the latter being true for $y=2$. Hence

$$Q_n>(2p_1)^{(p_2-1)\dots(p_s-1)}\div 2^{2^{s-2}}>p_1,$$

since at least $s-2$ of the primes p_2, ..., p_s exceed 2, so that the exponent is $\geqq 2^{s-2}$. For $s=2$, we have $p_1\geqq 3$, $Q_n>\frac{1}{2}y^{(p_1-1)(p_2-1)}\geqq p_1$ unless $p_1=3$, $y^{p_2-1}=2$, whence $p_2=2$, $y=2$, $n=6$, $x=2$.

Corollary. *If x is a positive integer >1, x^n-1 has a prime factor not dividing x^m-1 ($m<n$), except in the cases $n=2$, $x=2^k-1$; $n=6$, $x=2$.*

DEPARTMENTS.

SOLUTIONS OF PROBLEMS.

ALGEBRA.

Problems 219, 220 were also solved by L. E. Newcomb. No. 222 was also solved by A. H. Holmes.

223. Proposed by THEODORE L. DE LAND, Office of the Secretary of the Treasury, Washington, D.C.

An officer in the Treasury Department assigned three clerks to count a lot of silver dollars and when finished noted that there was an apparent difference in their efficiency; and, to determine the fact, gave to each a similar lot of the same amount to count, the only record made at the time being that A to count his lot alone, took three weeks longer, B took two weeks longer, and C took one week longer than it took for all working together to count the first lot. The best counter, on the record made, was given an efficiency mark of 93 on the scale of 100. What efficiency mark should, on the record, be given to each of the other two counters?

Solution by the PROPOSER.

Let x=the time for A, B, and C working together to finish one lot.

Then $x+3$=the time for A to finish one lot working alone;

$x+2$=the time for B to finish one lot working alone; and

$x+1$=the time for C to finish one lot working alone.

Then $\dfrac{1}{x}$=what A, B, and C can do in one week working together;

$\dfrac{1}{x+3}$=what A can do in one week working alone;

$\dfrac{1}{x+2}$=what B can do in one week working alone; and

$\dfrac{1}{x+1}$=what C can do in one week working alone.

Equating like terms we have,

$$\frac{1}{x}=\frac{1}{x+3}+\frac{1}{x+2}+\frac{1}{x+1}\text{.........}(1).$$